

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number  
**WO 2004/114123 A2**

(51) International Patent Classification<sup>7</sup>: **G06F 7/72**

Philips Intellectual Property & Standards, Cross Oak Lane,  
Redhill, Surrey RH1 5HA (GB).

(21) International Application Number:  
PCT/IB2004/001981

(74) Agent: **WILLIAMSON, Paul, L.**; c/o Philips Intellectual  
Property & Standards, Cross Oak Lane, Redhill, Surrey  
RH1 5HA (GB).

(22) International Filing Date: 10 June 2004 (10.06.2004)

(25) Filing Language: English

(81) Designated States (*unless otherwise indicated, for every  
kind of national protection available*): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,  
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,  
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,  
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,  
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,  
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,  
ZW.

(26) Publication Language: English

(30) Priority Data:  
0314562.0 21 June 2003 (21.06.2003) GB

(71) Applicant (*for all designated States except US*): **KONIN-  
KLJKE PHILIPS ELECTRONICS N.V.** [NL/NL];  
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

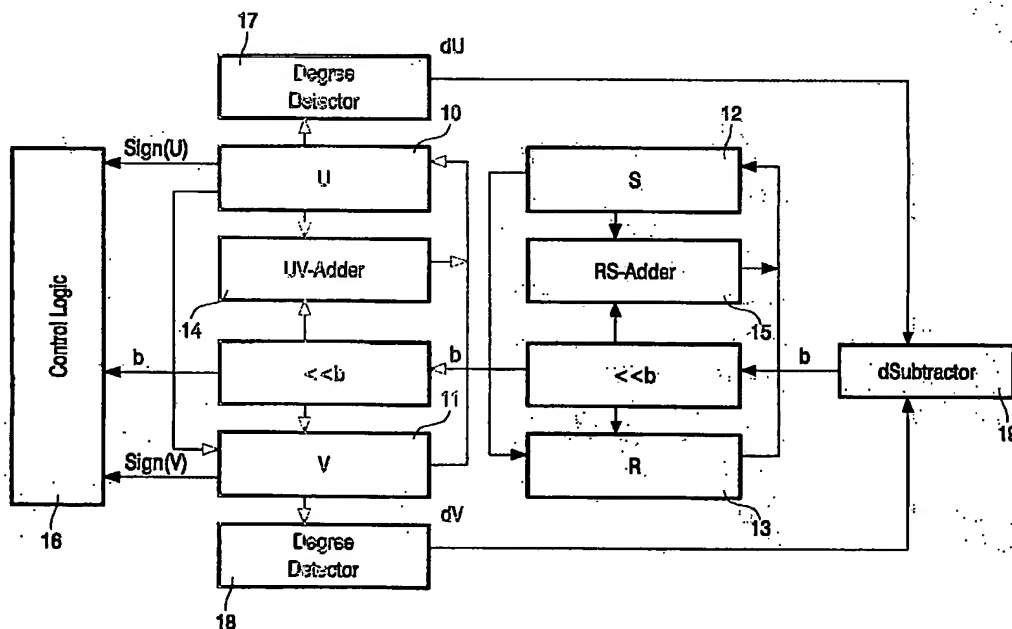
(84) Designated States (*unless otherwise indicated, for every  
kind of regional protection available*): ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,  
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **HUBERT, Gerar-  
dus. T., M.** [NL/NL]; c/o Philips Intellectual Property &  
Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA  
(GB). **VAN RIJNSWOU, Sander, M.** [NL/NL]; c/o

[Continued on next page]

(54) Title: **IMPROVED INVERSION CALCULATIONS**



(57) Abstract: An Elliptic Curve Cryptography inversion technique utilises operating on the MSW of four auxiliary variables U, V, R and S with specified invariances.



SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

**Declaration under Rule 4.17:**

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA,

**Published:**

- without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.